UNIVERSIDAD CARLOS III DE MADRID

PROYECTO FIN DE CARRERA

Protocolos Criptográficos de Intercambio Racional

Autor:
Román Ginés Almendros Mateo

Directora:
Dra. Dña. Almudena Alcaide Raya

Departamento de Informática

Leganés, Mayo 2011

Agradecimientos

Una vez finalizado este proyecto, se valora más la ayuda que he tenido para poder conseguirlo.

En primer lugar a mi mujer, María José, no solo por el tiempo que he estado desaparecido de casa, sino por su apoyo y sobre todo saberme escuchar en los malos momentos.

A mis hijas Valeria y Ariadna, que sin comprender lo que su padre hacía, aguntaron las dos delante del ordenador en lugar de jugar en el parque.

A mi tutora Almudena Alcaide Raya, que veía luz y esperanza cuando yo veía sombras y desazón.

La lista puede aumentarse con más nombres propios, pero no quisiera olvidarme de mis amigos y familia que han escuchado mis batallas del proyecto desde el pirncipio hasta el final.

Resumen

Este proyecto sobre Protocolos Critográficos de Intercambio Racional, continúa con el camino abierto por la Dra. Almudena Alcaide Raya en su tesis doctoral "Rational Exchange Protocols". En este trabajo nos hemos centrado en un problema concreto que surgía al realizar aleatoriamente algunos experimentos: la imposibilidad de encontrar *soluciones racionales* a problemas concretos de intercambio. Por lo tanto, la búsqueda de un resultado que nos indicara cuándo se iba o no a obtener un protocolo *racional* era fundamental. Ante la ausencia de una TTP (tercero de confianza) que controlara el intercambio *justo*, teníamos que formalizar aquellos escenarios en los que sí era posible llevar a cabo un intercambio *racional* y aquellos otros en los que no era factible.

Con el modelo matemático propuesto, basado en Teoría de Juegos y el Equilibrio de Nash, hemos definido un conjunto de matrices (de Estado, de Beneficio y de Relaciones) que nos posibilita el traducir un problema de intercambio entre entidades, en un problema matricial. Este formalismo también nos ha facilitado la definición de una taxonomía en la que emergen dos conceptos importantes: los incentivos y las coaliciones. El prinicipal resultado obtenido matemáticamente indica que, *ante la ausencia de incentivos o coaliciones en un protocolo de intercambio, sucede que dicho protocolo no es racional*. En otras palabras, si varias entidades quieren intercambiar determinados items o fichas entre ellas, y no existe un sistema de incentivos o de coaliciones, ante la no presencia de una TTP, las entidades prefieren no intercambiar, por miedo a perder lo que tenían o no obtener lo que querían. Gracias a estos sistemas de incentivos o de coaliciones, las entidades saben que aunque en algún instante del protocolo lleguen a acumular alguna pérdida con respecto a lo que tenían o querían, al final se les asegura que obtendrán un beneficio mayor del que partieron.

Dado que este resultado era demasiado teórico buscamos un escenario de aplicación. Lo encontramos en los *Intercambios Vacacionales*, que actualmente se realizan a través de una TTP llamada RCI. La relación con el resultado teórico es la siguiente: si varias entidades desean intercambiar vacaciones, nadie dará el primer paso pensando que no va a obtener lo que quiere o que va a perder lo que tiene. El modelo matemático que formaliza este entorno nos permite determinar en qué condiciones o qué restricciones se deben imponer para que el intercambio vacacional se lleve a cabo. Es decir, que al final de todo el protocolo cada entidad quede satisfecha y no haya motivos para que ningún participante se desvíe de cada paso dictado por el protocolo de intercambio. En nuestros experimentos hemos restringido ciertas variables de negocio, para así poder manejar la aplicación que hemos desarrollado, y que los resultados fueran fácilmente interpretables.

Índice

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

Un protocolo de seguridad de *intercambio justo* es un protocolo criptográfico que permite que varias entidades intercambien items/fichas, de tal manera que, aún cuando una o más entidades se aparten de la descripción del protocolo, ninguna de las entidades terminará en una situación de desventaja; es decir, no hay entidades que, después de haber enviado sus elementos no hayan recibido los adecuados a dicho cambio.

El interés en esta clase de protocolo se deriva de su importancia en muchos servicios actuales como la firma de contratos digitales, certificados de correo electrónico, comercio electrónico, etc. Por otra parte, la garantía de la equidad es fundamental cuando los elementos intercambiados incluyen cualquier tipo de evidencia de no repudio, ya que esto constituye un servicio clave en la mayoría de las ya mencionadas aplicaciones.

Desafortunadamente, no existe un protocolo por el cual un número de entidades puedan intercambiar item/fichas de manera justa, exclusivamente por ellos mismos, suponiendo que entidades deshonestas también participen en el protocolo. Pagnia y Gartner proporcionan un tratamiento formal de este resultado de imposibilidad en [Pagnia and Gärtner, 1999]. La idea intuitiva, evitando esbozar los detalles técnicos, sería: durante la ejecución del protocolo, una de las entidades tiene que ser la primera en el intercambio de su item/ficha a otra entidad. En ese momento, la primera entidad cae en una situación injusta que una entidad con un mal comportamiento puede aprovechar. Por lo tanto, el protocolo más simple que puede proporcionar la verdadera justicia se basa en el uso de una tercera entidad de confianza o TTP. El papel de la TTP varía de una clase a otra de protocolos de intercambio justo,

en función de su participación. En los sistemas basados en una TTP *in line* (por ejemplo, [Bahreman and Tygar, 1994]), la TTP, como autoridad de confianza, está involucrada en todos los mensajes intercambiados. En una TTP *on line* (por ejemplo, [Abadi et al., 2002]), la TTP está involucrada en la ejecución de cada protocolo, pero no necesariamente en todos los mensajes intercambiados entre las partes. Un tercer paso hacia la reducción del papel de la TTP fue la introducción de TTP *off-line* (véase [Asokan et al., 1997, Asokan et al., 1998]). En estos protocolos, denominados *intercambio óptimo justo*, las entidades tratan de llevar a cabo el intercambio por ellas mismas, y solo se recurre a la TTP en caso de un mal comportamiento de una de las entidades deshonestas, o cuando se produce un error durante la ejecución del protocolo.

Sin embargo, los últimos paradigmas de computación (por ejemplo, ad hoc y peer-to-peer (P2P)) plantean un desafío desde el punto de vista de la seguridad, ya que no es realista suponer que los servicios como los proporcionados por una TTP estarán disponibles en estos ambientes. En este contexto, el concepto de *intercambio racional* se convierte de gran interés,ya que los protocolos de intercambio racional tienen la principal ventaja de no necesitar un TTP.

En 1998, P. Syverson introdujo la idea de *intercambio racional* como una alternativa a *intercambio equitativo o justo* de los escenarios en los que el uso de un TTP no se permite o no es viable ([Syverson, 1998]). Un protocolo de seguridad de intercambio racional es un protocolo criptográfico que permite que varias entidades intercambien item/fichas, de tal manera que, si una o más entidades se apartan de la descripción del protocolo y dejan en desventaja a otros participantes, aquellos no pueden obtener ninguna ventaja al hacerlo. Informalmente, un protocolo de intercambio racional no puede proporcionar justicia, sino que tiene que asegurar racionalidad (es decir, los intereses propios de cada entidad han de ser satisfechos al final del protocolo). En otras palabras, ninguna entidad unilateralmente tendría razón para apartarse del protocolo, pues un mal comportamiento no resultará en un beneficio directo.

Por último, en 2001 Buttyán et al. identifican los principios de la Teoría de Juegos, como una herramienta poderosa y conveniente para analizar los protocolos de intercambio racional ([Buttyán and Hubaux, 2001], [Buttyán, 2001]). Más recientemente, algunos esfuerzos se centraron en

ampliar el modelo de Buttyán para el análisis formal de protocolos de intercambio racional en situaciones más complejas [Alcaide et al., 2006, Alcaide et al., 2007, Palomar et al., 2007].

1.1. Motivación

1. Cada vez hay más entornos reales en los que no es posible un intercambio justo, se necesitan otros esquemas de intercambio.

2. No existen resultados formales que permitan razonar y analizar escenarios de intercambio racional.

3. La eliminación de las TTP reduce los costes de las operaciones o transacciones comerciales.

4. Un entorno de aplicación directo a redes ad-Hoc y sistemas P2P descentralizados, cada vez más extendidos.

1.2. Nuestro Enfoque

En trabajos anteriores ([Alcaide et al., 2008a, Alcaide et al., 2008b, Alcaide, 2009]) se describe un formalismo para la síntesis automática de protocolos de seguridad de intercambio racional multi–parte (M-RES protocolos). Las principales propiedades del formalismo se resumen a continuación:

- Dado un problema de intercambio, el formalismo hace uso de sencillas estructuras lineales, tales como vectores y matrices, para representar todos los aspectos del problema (número de entidades, fichas que pueden cambiarse, el valor de las fichas, las entidades, posesiones iniciales, etc)

- El modelo es muy flexible y escalable para entornos con cualquier número de agentes participantes. En el formalismo, se consideran sólo entidades racionales (egoístas) que buscan su mayor beneficio.

- Para cualquier problema de intercambio, el modelo define un marco adecuado para el uso de técnicas heurísticas en la búsqueda de soluciones racionales.

- Por último, el sistema de prueba se basa en los resultados de la Teória de Juegos .

  Las demostraciones de racionalidad se basan en el cálculo del equilibrio de Nash por inducción hacia atrás.

En este trabajo, extendemos el formalismo anterior:

- Proporcionando una manera fácil de representar conceptos tradicionalmente muy complejos, como los incentivos y las coaliciones entre las entidades que intercambian.

- Definición de una taxonomía para clasificar los protocolos M-RES basados en:

  1. Identificar si los participantes del protocolo son parte de cualquier plan de incentivos que hacen que se comporten de cierta manera predeterminada.
  2. Identificar si los participantes son miembros de una coalición.

- Por último, se presenta un resultado que describe *"la imposibilidad de diseñar un protocolo racional para cualquier propuesta de problema de intercambio entre entidades, con la ausencia de incentivos y coaliciones entre los participantes"*. Se dará una prueba formal de este resultado.

  El resultado de imposibilidad, aquí descrito, es de gran importancia para los *Problemas de Intercambio*, ya que establece que, en ausencia de un TTP (entonces no es posible un intercambio justo), solo a través de programas de incentivos o de grupos de coaliciones, pueden varias entidades no cooperativas intercambiar item/fichas de una manera racional . En otras palabras, en ambientes sin estructura (no disponible TTP), las entidades no cooperativas pueden realizar un intercambio, solo cuando esas entidades estan incentivados a hacerlo o cuando se forman grupos de coalición entre ellos. El término no cooperación se aplica para designar entidades egoistas, interesadas en su propio beneficio. Una entidad no cooperativa siempre tiene la necesidad de los agentes externos (incentivos o coaliciones) para realizar un intercambio, en la ausencia de los servicios que por lo general desplegaba una TTP.

El resultado es aplicable a los protocolos diseñados para el intercambio de tokens de no repudio, los sistemas P2P de intercambio de archivos, la firma de contratos, computación multi-parte, e-comerce, etc.

Otras consecuencias de este resultado se dan en la aparición de un comportamiento cooperativo. Algunos resultados teóricos, en los campos de la Teoría de Juegos y la Teoría de Juegos Evolutiva, establecen que la cooperación puede surgir naturalmente en escenarios de problemas de intercambio entre entidades, como se indica en [Aumann, 1959, Aumann, 1960, Aumann, 1961, Maynard-Smith and Price, 1973]. Con respecto a los protocolos de intercambio racional, podemos describir dos escenarios posibles : (1) que en repetidas ocasiones, el mismo protocolo es ejecutado con el mismo conjunto de entidades y, (2) cuando el mismo protocolo, se repite varias veces, pero las entidades no son necesariamente las mismas en cada iteración. El resultado de imposibilidad que aquí se presenta establece formalmente que la cooperación entre las entidades de un problema de intercambio no puede surgir de forma natural, a menos que los factores externos, como los incentivos o coaliciones, sean implementados.

1.3. Objetivos

1. Desarrollar un modelo matemático que nos permita razonar formalmente sobre los problemas de intercambio racional.

2. Búsqueda de un resultado teórico que nos indique cuándo y sobre qué condiciones, va a existir un protocolo de intercambio racional.

3. Diseñar un entorno de aplicación, donde visualicemos de forma práctica el resultado anterior.

1.4. Organización por Capítulos

El documento está organizado de la siguiente manera.

- En el capítulo 2, ***Fundamentos del Modelo***, se describe brevemente el formalismo que nos permitirá definir los incentivos y las coaliciones.

- En el capítulo 3, ***Taxonomía***, se presenta la taxonomía de los protocolos M-RES, atendiendo a estas definiciones.

- En el capítulo 4, ***Imposibilidad del Intercambio Racional***, se dedica a la prueba formal del resultado de la imposibilidad de intercambio racional para determinados problemas de intercambio.

- En el capítulo 5, ***Entorno de Aplicación***, presentamos el entorno de aplicación práctico elegido, basado en Intercambios Vacacionales o Multipropiedad.

- En el capítulo 6, ***Conclusiones*** indicamos las principales conclusiones de este trabajo.

- Por último, en el anexo A, ***Presupuesto del Proyecto***, se valora económicamente la realización de dicho proyecto.

Capítulo 2

Fundamentos del Modelo

En esta capitulo presentamos un resumen del formalismo descrito previamente en [Alcaide et al., 2008a, Alcaide et al., 2008b, Alcaide, 2009]. Por favor refiérase a la bibliografía para más detalles.

2.1. Protocolo de Intercambio.

Formalmente, se define un protocolo de intercambio de la siguiente manera:

Definición 2.1.1 (Protocolo de Intercambio)**.** *Definimos un protocolo de intercambio entre entidades como la tupla* $\Pi = \langle P, \mathcal{O}, T \rangle$ *donde:*

- $P = \{P_0, \ldots, P_{v-1}\}$ *es el conjunto de las entidades participantes en el protocolo,*
- $\mathcal{O} = \{o_0, \ldots, o_{m-1}\}$ *es el conjunto de todos los item/fichas que se intercambian durante la ejecución del protocolo, y*
- T *es una colección ordenada de n pasos, que describe el esquema del protocolo, cada uno de la siguiente forma:*

$$(stp_t) \quad P_i \rightarrow P_j : o_{t_1}, \ldots, o_{t_{k_t}} \tag{2.1}$$

cuando:

- $\{stp_0, \ldots, stp_{n-1}\}$ *son los números de cada paso.*
- P_i, $P_j \in P$, $i \neq j$, *es el emisor y el receptor del mensaje, respectivamente.*

$$S^{\pi} = \begin{pmatrix} emisor & receptor & o_0 & o_1 & o_2 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Figura 2.1: Ejemplo de una matriz protocolo.

- $\{o_{t_1}, \ldots, o_{t_{k_t}}\} \in \mathcal{O}$ *son los elementos que* P_i *envía a* P_j*, sujeto a que la entidad* P_i *posea los elementos en el paso* stp_t *del protocolo.*

Téngase en cuenta que esta definición no menciona la racionalidad, la equidad o la viabilidad del intercambio. Se limita a describir una serie de mensajes que se intercambian entre los participantes. Al final de la ejecución del protocolo, algunas entidades han perdido el control sobre algunos de sus elementos (item/fichas), así como han obtenido acceso a otros nuevos.

Los protocolos descritos en la definición 2.1.1 estarán representados como se describe en el siguiente Sección.

2.2. La Matriz del Protocolo.

Un protocolo Π es representado por una matriz $S^{\Pi} \in \mathcal{M}_{n\times(m+2)} = [s^{\Pi}_{i,j}]$, de números enteros, donde se interpreta cada fila como un mensaje en el que los dos primeros componentes identifican el emisor y el receptor del mensaje, respectivamente, y el resto de los componentes de la fila representan los elementos que se envían (un 1 cuando el emisor tiene que enviar ese item/ficha al receptor y 0 en caso contrario) .

A modo de ejemplo, la matriz que se muestra en la Fig. 2.1 representa un protocolo de tres pasos de intercambio que involucra a tres entidades. En el paso cero, la entidad P_0 envía a la entidad P_1 el item/ficha o_0 entonces, la entidad P_1 envía a la entidad P_2 el item/ficha o_1 y, por último, en el paso dos, P_2 envía a la entidad P_0 los item/ficha o_1 y o_2.

A pesar de que la matriz S^{Π} representa la serie de pasos que las entidades participantes tienen que tomar a lo largo de la ejecución de un protocolo, el contenido real del verdadero mensaje que se envió a cada paso está sujeto a: (1) la entidad remitente posee los elementos, y (2) aquellos elementos que son accesibles a ese remitente. Diferentes situaciones pueden derivar en un estado de *no acceso* a un elemento o_j para una entidad en particular P_i. Por

ejemplo, si un elemento o_j está cifrado y la entidad P_i no tiene la clave de descifrado. Algo similar ocurre si la entidad P_i es capaz de generar el elemento o_j pero es necesario tener acceso a otros elementos para hacerlo. En este caso, el item/ficha o_j debe seguir siendo de no acceso hasta obtener el control sobre el resto de los item/fichas necesarios. Durante la ejecución del protocolo, este tipo de información, que es específica para el problema de cambio particular en cuestión, se plasmarán en dos matrices adicionales: una matriz $H(t)$ denota *el estado* y una matriz de R, que denota *la dependencia* que describen las relaciones entre las entidades. Ambas estructuras se describen a continuación.

2.3. Matriz Estado

La matriz $H(t) = [h_{i,j}(t)] \in \mathcal{M}_{v\times m}$ captará las posesiones de cada una de las entidades, en las diferentes etapas de la ejecución del protocolo, $t \in \{0, \ldots, n\}$. La matriz denotada por $H(0)$ representa las posesiones de cada entidad diferente en el punto inicial, esto es, antes de iniciarse el intercambio. $H(1)$ representará las pertenencias tras el paso stp_0 del protocolo y, por último, $H(n)$ capturará las posesiones de las entidades después de la etapa final stp_{n-1}.

$$h_{i,j}(t) = \begin{cases} \texttt{ACC} & \text{si y sólo si } P_i \text{ posee y tiene acceso completo al item/ficha } o_j \\ \texttt{NO\_ACC} & \text{si y sólo si } P_i \text{ posee el item/ficha } o_j \text{ pero no tiene acceso a ella} \\ \texttt{LOST} & \text{si y sólo si } P_i \text{ ha perdido el control sobre el item/ficha } o_j \\ \texttt{UNKNO} & \text{si y sólo si } o_j \text{ desconoce a la entidad } P_i \end{cases} \tag{2.2}$$

Tenga en cuenta que el valor $h_{i,j}(0)$ no podrá ser establecido como `LOST` ya que no ha podido perderse ningun item, por parte de una entidad, en $t = 0$.

Por otra parte, los siguientes son los valores numéricos posibles de cada uno de los elementos, en la Matriz Estado. Estos valores nos permiten calcular beneficios parciales y finales para cada entidad con un simple producto escalar de vectores. Los valores son:

`ACC` =	1	Multiplicado por un valor de ganancia incrementará la utilidad total.
`UNKNO` =	0	Multiplicado por un valor de ganancia se anulará la utilidad total.
`LOST` =	-1	Multiplicado por un valor de ganancia se disminuirá la utilidad total.

(2.3)

$$H(0) = \begin{pmatrix} o_0 & o_1 & o_2 \\ \texttt{ACC} & \texttt{UNKNO} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{NO\_ACC} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{UNKNO} & \texttt{ACC} \end{pmatrix}$$

Figura 2.2: Ejemplo de una matriz estado.

El estado `NO_ACC` puede tomar cualquier valor diferente de los anteriores. Este estado servirá para anular la utilidad hasta que un determinado evento se lleve a cabo y nunca se multiplica por el valor de ganancia correspondiente.

A modo de ejemplo, la matriz $H(0)$ que se muestra en la Fig. 2.2 representa una matriz de estado inicial en la que una entidad P_0 tiene acceso al item/ficha o_0. Por el contrario, la entidad P_1 posee el item/ficha o_1 pero no tiene acceso a ella, y P_2 tiene acceso al item/ficha o_2.

La no accesibilidad indica que puede haber relaciones de dependencia entre los diferentes elementos que poseía, así como entre los elementos que tienen las diferentes entidades. Una matriz R captará las relaciones de dependencia de cada elemento de la matriz de estado H y para el problema de cambio particular en la mano.

2.4. Matriz de Dependencias.

Una matriz $R = [r_{i,j}] \in \mathcal{M}_{(v\times m)\times(v\times m)}$ capturará la interrelación de dependencia por cada $h_{i,j} \in H$ para un problema de intercambio determinado. Dos tipos diferentes de relaciones de dependencia, *positiva* y *negativa*, se puede expresar en el modelo de la siguiente manera:

- los items o_i y o_j están positivamente relacionados, si cuando o_j no es de acceso, a continuación, acceder a o_i implica acceder al item o_j también.
- los items o_i y o_j tienen un efecto negativo si cuando o_j no es de acceso, despues de recibir o_i implica hacer el item o_j de no acceso.

Otros vínculos de dependencia más complejos pueden ser representados en la matriz R, con la participación de varios elementos. La única restricción impuesta por esta representación es que las relaciones positivas y negativas entre dos elementos dados no pueden ser expresadas al mismo tiempo.

2.5. Actualización de la Matriz de Estado para el Remitente de un Mensaje.

Teniendo en cuenta la matriz de un protocolo S^{Π}, la matriz estado $H(0)$, y una matriz de relaciones de dependencia R, queda especificado el escenario del intercambio. Cuando avanza la ejecución del protocolo, la matriz estado H se actualiza conforme a las instrucciones dadas en el protocolo y las restricciones positivas y negativas impuestas por la matriz de R. Al final de la ejecución del protocolo $H(n)$ reflejará las posesiones que cada entidad tiene y también los elementos de los que cada entidad ha perdido el control.

Habida cuenta que (stp_t) $P_s \rightarrow P_r : \{o_l\}$, define un paso del protocolo representado por una matriz S^{π}, $(t \in \{0, \ldots, n-1\})$. La siguiente expresión (2.4) sirve para designar formalmente la actualización del estado de la matriz $H(t)$ para la entidad remitente P_s después del paso (stp_t). $H(t+1)$ es el resultado de esta actualización, y cada elemento$h_{s,l}(t+1)$ representa las posesiones de los participantes P_s.

$$\begin{array}{l} \text{Si } h_{s,l}(t) = ACC \Rightarrow h_{s,l}(t+1) = LOST \\ \text{Si } h_{s,l}(t) \neq ACC \Rightarrow h_{s,l}(t+1) = h_{s,l}(t) \end{array} \tag{2.4}$$

Un algoritmo similar se define para el destinatario de un mensaje, a pesar de otras consideraciones en relación con la dependencia de los item/fichas.

2.6. Matriz de Beneficio.

En nuestro modelo, todos los participantes asignan un valor particular a cada item/ficha involucrado en el intercambio. Este valor depende de si esa entidad está interesada en acceder a ese item, si aumenta el coste para la entidad mediante el envío de ese item/fivha, o para mantenerlo. Estos valores también sirven para representar a la persona, estableciendo los requisitos y que han sido definidos en la siguiente matriz.

$$B = \begin{pmatrix} o_0 & o_1 & o_2 \\ \texttt{COST} & \texttt{NO\_COST} & 5 \\ 3 & \texttt{COST} & \texttt{NO\_COST} \\ \texttt{NO\_COST} & 3 & \texttt{BENEF} \end{pmatrix}$$

Figura 2.3: Ejemplo de una matriz de beneficios.

Matrix $B = [b_{i,j}] \in \mathcal{M}_{v\ timesm}$ se define como:

$$b_{i,j} = \begin{cases} \texttt{COST} & \text{si y sólo si } P_i \text{ incurre en costes al perder el control sobre el item } o_j \\ \texttt{NO\_COST} & \text{si y sólo si } o_j \text{ no tiene ningún valor para las entidades } P_i \\ \texttt{BENEF} & \text{si y sólo si } P_i \text{ obtiene beneficios al perder el control del item } o_j \\ > 1 & \text{si y sólo si } o_j \text{ es requerido por la entidad } P_i \end{cases} \tag{2.5}$$

En el caso de b_{ij} mayor que uno, b_{ij} también representa el valor que ese elemento o_j vale la pena para la entidad P_i si y sólo si o_j se hace accesible para P_i .

Los siguientes valores numéricos asignados a cada elemento de la matriz B nos permitirá calcular los beneficios parciales y finales de las entidades, multiplicando cada fila de las matrices H y B. Los valores son:

$$\begin{aligned} \texttt{COST} &= \quad 1 \\ \texttt{NO\_COST} &= \quad 0 \\ \texttt{BENEF} &= -1 \end{aligned} \tag{2.6}$$

A modo de ejemplo, la matriz B se muestra en la Fig.2.3 representa una matriz de Beneficio en la que la entidad P_0 aumentó sus costos al perder el control sobre el tema o_0 con un valor de cinco unidades del item o_2. De manera similar, el item o_0 es equivalente a tres unidades para la entidad P_1 y perder el control sobre el item o_1 tiene un coste para P_1 . Por último, la entidad P_2 tiene un valor de tres unidades para o_1, mientras que la perdida del item o_2 no resulta rentable.

2.7. Beneficio de las Entidades y Diferencial de Rentabilidad

En cada paso del protocolo (después de actualizar la matriz estado), podemos calcular los logros alcanzados por un jugador hasta la fecha y nos referimos a estos valores como ütilidad.º "pagos".

Definición 2.7.1 (Beneficio de las Entidades)**.** *Teniendo en cuenta un protocolo matriz de la forma S^{Π}, el valor de beneficio para los entidades participantes P_i después del paso stp_t, ($0 \leq t \leq n-1$), se puede calcular como:*

$$u_i(t+1) = \sum_{\substack{j=0 \\ h_{i,j} \neq \texttt{NO\_ACC}}}^{m-1} b_{ij} * h_{ij}(t+1), \quad i \in \{0, \ldots, v-1\} \tag{2.7}$$

Tenga en cuenta que la expresión (2.7) incluye implícitamente el coste inducido por la pérdida de control sobre un item de valor. Cuando P_i envía o_k, h_{ik} pasa de $+1$ a -1, y por lo tanto la utilidad total se reduce en $2b_{ik}$.

Tenga en cuenta que, $u_i(0)$ denota la utilidad inicial para la entidad P_i, $u_i(1)$ representa la recompensa del participante P_i después del paso stp_0 del protocolo y $u_i(n)$ es el rentabilidad alcanzada por P_i después de que el último paso stp_{n-1}. También tengamos en cuenta, que los items/fichas de NO_ACC no aumentan la utilidad general.

Definición 2.7.2 (Diferencial de rentabilidad de la Entidad)**.** *Teniendo en cuenta una matriz de protocolo de la forma S^{Π}, el valor diferencial de rentabilidad para un jugador de P_i entre los pasos de t_1 y t_2, con $0 \leq t_1 \leq t_2 \leq n$, se define como :*

$$du_i(t_1, t_2) \quad = u_i(t_2) - u_i(t_1) \tag{2.8}$$

Durante la ejecución de un protocolo, puede haber etapas en las que los jugadores están temporalmente en un estado peor (es decir, $du_i(t, t+1) \leq 0$). Sin embargo, el hecho relevante es si al final del protocolo, cada entidad P_i obtiene utilidad diferencial suficiente:

- Si $du_i(0, n) > 0$, el intercambio es rentable para P_i,

- Si $du_i(0,n) < 0$, el intercambio no es rentable para P_i,
- Si $du_i(0,n) = 0$, el intercambio no es de ninguna utilidad para P_i,

2.8. El Espacio de Soluciones

Dado un problema de intercambio definido por las matrices B (de beneficios), $H(0)$ (estado inicial) y R (de dependencias), el formalismo que acabamos de describir se utiliza para representar un problema. A falta de una TTP, una solución racional es necesaria. Un protocolo de intercambio racional Π, representado por la matriz S^{Π}, da solución al problema descrito si se cumplen los siguientes requisitos:

1. **Viabilidad:** Es decir, el intercambio descrito por el protocolo Π representa una transferencia posible entre los participante del protocolo, de los elementos necesarios ,
2. **Racionalidad:** El protocolo Π es racional. Es decir, durante la ejecución de un protocolo, puede haber etapas en las que los jugadores están en un estado temporal "peor"(es decir, $du_i(t,t+1) \leq 0.$), sin embargo, las siguientes propiedades deben ser alcanzadas :
   - A final de la ejecución del protocolo, cada participante P_i debe haber ganado utilidad diferencial suficiente. En otras palabras, para cada participante, la utilidad diferencial total $du_i(0,n) > 0$, debe estar por encima de un mínimo requerido. Este mínimo se calcula utilizando el beneficio representado en la matriz B. Por favor refiérase a la bibliografía extensa.
   - Por cada acción final de cada entidad en la ejecución de un protocolo (la última vez que una entidad es el remitente o el destinatario de los mensajes), el beneficio alcanzado por la acción directa debe aumentar su pago directamente .

2.8.1. Número Total de Protocolos de Intercambio que Existen

Como se describe en la sección 2.2, un protocolo es representado por una matriz $S^{\Pi} \in \mathcal{M}_{n\times(m+2)}$. Una estimación del número total de protocolos de

intercambio posibles, viene dada por:

$$\mathcal{O}\big(\frac{v!}{(v-2)!}2^{nm}\big) = \mathcal{O}\big(v(v-1)2^{nm}\big) = \mathcal{O}(v^2 2^{nm}) \tag{2.9}$$

donde n es el número de pasos de protocolo, v es el número de entidades y m es el número de fichas que participan en el intercambio.

Es difícil determinar cuántos de estos protocolos representan *soluciones factibles* a un problema de intercambio específico. Aún más difícil es estimar cuántas de esas soluciones factibles representan un *intercambio racional* . Una búsqueda heurística basada en recorrido simulado se utilizó para encontrar los diseños de protocolo, en el espacio de solución de un determinado problema de intercambio entre entidades, que cumplan las anteriores condiciones de viabilidad y racionalidad ([Alcaide et al., 2008b, Alcaide, 2009]).

2.9. Incentivos y Coaliciones

En esta sección, se utiliza el modelo formal que acabamos de describir, en particular, la combinación de valores en la matriz estado H y la matriz de beneficio B, para clasificar protocolos M-RES.

Informalmente, en cualquier esquema de intercambio dado, una vez que los objetivos del intercambio se han alcanzado, la motivación para continuar se deriva en incentivos, sistemas de muchos tipos (factores de reputación, programas de fidelización, etc) y/o, la presencia de coaliciones entre las entidades participantes. De hecho, un plan de incentivos es un refuerzo externo artificial, para hacer que las entidades se comportan de cierta manera que, a priori, no parece ser racional. En un entorno donde las entidades son de interés propio y orientado a maximizar la utilidad de sus valores propios, un plan de incentivos siempre debe representar una prima sobre los valores de beneficio de las entidades. De manera similar, cuando una entidad es parte de una coalición, ayudando a los demás miembros de la misma coalición para lograr sus objetivos también debe reportar un aumento en los valores de ganancia de los miembros de la coalición.

En esta sección vamos a dar definiciones formales de estos conceptos (incentivos y coaliciones) y en el Capítulo 3 vamos a clasificar a las entidades de acuerdo a estos conceptos.

2.9.1. Esquema de Incentivos

Por definición, un sistema de incentivos es *un mecanismo formal para inducir a alguien a hacer algo*. Dentro de nuestra taxonomía, un sistema de incentivos es considerado como un mecanismo por el cual las entidades están motivadas para intercambiar *sus propios* artículos.

Por lo general, los participantes de un protocolo de intercambio son impulsados por el deseo de acceder a los elementos necesarios y estará ansioso por recibirlos. Un plan de incentivos motivará a los participantes a perder el control sobre los elementos de su propiedad, por lo que otras entidades puedan tener acceso a ellos. El incentivo representa una prima sobre su pago si sus propios artículos se envían a los demás participantes. Por ejemplo, un correo electrónico de buena reputación - el comerciante enviará el mensaje correspondiente, después de recibir el pago de un comprador por las mercancías, ya que su negocio futuro podría depender del resultado de la transacción actual. En este caso, un plan de incentivos podría ser un sistema de reputación externa obligando a los comerciantes a comportarse con honestidad en cada transacción.

Por lo general, los participantes de un protocolo no son motivados por el mismo factor de incentivo . Algunos participantes del protocolo podrían estar motivados por un factor de prestigio, mientras que otros podrían responder a incentivos o castigos por aplicación de la ley. Además, una entidad podría ser incentivada hacia el intercambio de un elemento en particular, y puede no haber ningún incentivo en la pérdida de control sobre otro elemento.

Con respecto a esta definición de incentivos se formalizan los siguientes conceptos:

Definición 2.9.1 (Entidad Incentivada)**.** *Dada una entidad P_i y un elemento o_j, donde P_i inicialmente posee o es capaz de generar o_j, la entidad P_i está incentivada hacia el intercambio del item o_j, si P_i puede aumentar su valor de beneficio por la pérdida del control de o_j.*

En otras palabras, enviar el item/ficha o_j representa un beneficio para P_i.

Definición 2.9.2 (Entidad no Incentivada)**.** *Dada una entidad P_i y un elemento o_j, donde P_i inicialmente posee o es capaz de generar o_j, la entidad P_i es no incentivada hacia el intercambio del item o_j, si P_i disminuye el valor de beneficio por la pérdida del control sobre o_j.*

En otras palabras, enviar el item o_j representa un costo a P_i. Una entidad no incentivada está motivada para mantener el control sobre el item o_j.

Representación del Modelo de Incentivos

La representación de los incentivos en el modelo formal es el siguiente:

- Si $h_{i,j}(0)$=`ACC` o $h_{i,j}(0)$=`NO_ACC` (es decir, el item o_j pertenece a la entidad P_i en el estado inicial del protocolo o P_i será capaz de generar o_j en algún momento a lo largo de la ejecución del protocolo).

  En cualquier caso, el correspondiente $b_{i,j}$ valor tendrá la semántica siguiente:

  - Si $b_{i,j}$ = `BENF`, la entidad P_i es incentivado para realizar el intercambio del item/ficha o_j. Esto es, enviar el artículo o_j representa un aumento de P_i en su valor de recompensa.
  - Si $b_{i,j}$ = `COST`, la entidad P_i no está incentivada para realizar el intercambio del item/ficha o_j. Esto es, perder el control sobre el item/ficha o_j representa una disminución de P_i en su valor de recompensa.
  - Si $b_{i,j}$ = `NO_COST`, la entidad P_i es indiferente hacia el tema o_j.

Tengan en cuenta que si la entidad P_i pierde el control sobre un elemento o_j en el paso t en la ejecución del protocolo, disminuye su beneficio definido en la ecuación (2.7), en dos unidades. Por el contrario, si $b_{i,j}$ = `BENEF`, el valor de la ganancia aumenta en dos.

2.9.2. Esquema de Coaliciones

Por definición, un régimen de coalición se refiere *al estado que forma la combinación de varias entidades, de forma que actuan como un solo cuerpo de entidad*. Dentro de nuestra taxonomía, un esquema con coalición se considera un mecanismo por el cual las entidades están racionalmente obligadas a ayudar a las entidades coaliadas para alcanzar sus metas o beneficios. Esto se hace mediante el reenvío de los item de las entidades participantes, cuando estos son requeridos por miembros de la coalición.

Típicamente, podría haber diferentes coaliciones formadas entre varias entidades de un protocolo determinado, mientras que otras entidades podrían quedarse solas. Además, estas coaliciones pueden tener intersección entre ellas (una entidad que pertenece a más de una coalición) o pueden formar grupos desarticulados.

Con respecto a esta definición de coalición se formalizan los siguientes conceptos:

Definición 2.9.3 (Entidad Aliada)**.** *Una entidad P_i es una aliada de otra entidad P_j, si P_i puede aumentar su beneficio mediante la transmisión de los elementos exigidos por la entidad P_j, sujeto a que los recibió y que tiene acceso a ellos en algún momento anterior del protocolo.*

Tengan en cuenta que esto es solo en relación a los item que P_i no tiene previamente como propios o no es capaz de generarlos, sino a los item que se envían a P_i desde otras entidades. Una entidad aliada P_i de otra entidad P_j representa a una coalición entre las entidades P_i y P_j con respecto a todos los elementos requeridos por cada uno de ellos.

Definición 2.9.4 (Entidad NO Aliada)**.** *Una entidad P_i es no aliada de otra entidad P_j, si P_i disminuye el valor de beneficio mediante el envío de los items que P_j necesita haber recibido o haber tenido acceso a ellos, en algún momento anterior del protocolo.*

En otras palabras, si las entidades P_i y P_j no forman parte de una coalición,la pérdida del control sobre los items requeridos, una de la otra, representan una disminución en sus valores de beneficio.

Representación de los Sistemas de Coalición

La representación de las coaliciones en el modelo formal es el siguiente:

- Si $h_{i,j}(0) = \texttt{UNKNO}$ (es decir, el item o_j no lo conoce la entidad P_i en el estado inicial del protocolo).

  El correspondientes valor $b_{i,j}$ tendrá la semántica siguiente:

  - Si $b_{i,j} > 1$, el item o_j es uno de los item exigidos por la entidad P_i y $b_{i,j}$ representa el valos del elemento o_j para la entidad P_i.

- Si $b_{i,j} =$ `BENEF`, la entidad P_i es parte de una coalición con cualquier entidad que requiere el item o_j.
- Si $b_{i,j} =$ `COST`, P_i entidad no forma parte de una coalición con cualquier entidad que requiere el item o_j.
- Si $b_{i,j} =$ `NO_COST`, entidad P_i es indiferente hacia el reenvío del item o_j.

Tengan en cuenta que si P_i no es parte de una coalición con la entidad P_k, y está requiere el item o_j, entonces el reenvío del item o_j representa un costo para la entidad P_i de acuerdo a la ecuación (2.7). Por el contrario, si P_i y P_k son aliados, y P_i tiene la oportunidad de enviar hacia adelante el item o_j requerido por la P_k, entonces P_i obtiene inmediatamente un beneficio mayor.

Capítulo 3

Taxonomía

3.1. Taxonomía para los Protocolos M–RES

Los protocolos de intercambio racional pueden ser tipificado según los diferentes tipos de entidades que participan en el intercambio. Nuestra taxonomía se basa en la identificación de dos aspectos principales: (1) si las entidades están incentivadas y (2) si son parte de una coalición. Estos criterios definen los diferentes tipos de entornos en los que se ejecuta un protocolo.

La combinación de los valores de la matriz de estado inicial $H(0)$ (Ecuación (2.2)) y la matriz de beneficio B (Ecuación (2.5)) se utilizan para representar y identificar los diferentes tipos de entidad. Las ecuaciones 2.2 y 2.5 dán la semántica a los diferentes valores que estas matrices podrían obtener durante la ejecución del protocolo. En esta sección vamos a añadir significado a todas las combinaciones posibles de estos valores (tabla 3.1).

3.1.1. Clasificación atendiendo a Incentivos

Simétrico Incentivado. Todos los participantes son racionales y parten de un plan de incentivos de un tipo u otro. Es decir, todas las entidades obtienen una rentabilidad positiva, cuando pierden el control sobre cada uno de sus propios productos.

Formalmente se puede representar este tipo de entorno de la siguiente

Tabla 3.1: Tabla de Incentivos y Coaliciones.

	$b_{i,j} = \texttt{NO\_COST}$	$b_{i,j} = \texttt{COST}$	$b_{i,j} = \texttt{BENEF}$	$b_{i,j} > 1$
$h_{i,j}(0) = \texttt{ACC} \vee$ $h_{i,j}(0) = \texttt{NO\_ACC}$	P_i indiferente al intercambio	P_i no incentivada para intercambiar o_j	P_i Incentivada para intercambiar o_j	NO–aplicable
$h_{i,j}(0) = \texttt{UNKNO}$	P_i indiferente a la obtención o_j	P_i no coaliado con P_k si P_k requiere o_j	P_i coaliado con P_k si P_k requiere o_j	Item o_j requerido por P_i

manera:

$$\begin{gathered} \forall i \in \{0, \ldots, v-1\} \quad y \quad \forall j \in \{0, \ldots, m-1\} \\ (h_{i,j}(0) = \texttt{ACC} \vee h_{i,j}(0) = \texttt{NO\_ACC}) \Rightarrow b_{i,j} = \texttt{BENEF} \end{gathered} \tag{3.1}$$

Simétrico NO Incentivado. Todas las entidades son racionales y aumentan sus costos al perder el control sobre sus propios artículos.

Formalmente se puede representar este tipo de entorno de la siguiente manera:

$$\begin{gathered} \forall i \in \{0, \ldots, v-1\} \quad and \quad \forall j \in \{0, \ldots, m-1\} \\ (h_{i,j}(0) = \texttt{ACC} \vee h_{i,j}(0) = \texttt{NO\_ACC}) \Rightarrow b_{i,j} = \texttt{COST} \end{gathered} \tag{3.2}$$

Asimétrico con respecto a Incentivos. Todas las entidades son racionales, pero algunas entidades podrían estar incentivadas con respecto a uno o más de sus elementos, así como habrá entidades que no esten todas incentivadas.

Ejemplos

Para ilustrar la clasificación anterior, se considerará el siguiente ejemplo: un escenario con dos entidades, cada entidad en posesión de un solo producto que es requerido por el otro participante. Además, un valor arbitrario $val_1 = 3$

es elegido para representar el valor que tiene para la entidad P_0 el producto o_1 y el valor de $val_2 = 5$ se corresponde con lo que el producto o_0 tiene de valor para la entidad P_1.

Las siguientes matrices son las del estado inicial y de beneficio, que representan el problema de intercambio descrito:

$$H(0) = \begin{pmatrix} \texttt{ACC} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{ACC} \end{pmatrix} \quad B = \begin{pmatrix} - & val_1 \\ val_2 & - \end{pmatrix} \tag{3.3}$$

Por último, las siguientes matrices $H(t)$ son la secuencia de ejecutar un protocolo, en el que P_0 envía a P_1 el item o_0 y P_1 envía a P_0 el item o_1:

$$H(0) = \begin{pmatrix} \texttt{LOST} & \texttt{UNKNO} \\ \texttt{ACC} & \texttt{ACC} \end{pmatrix} \quad H(1) = \begin{pmatrix} \texttt{LOST} & \texttt{ACC} \\ \texttt{acc} & \texttt{LOST} \end{pmatrix} \tag{3.4}$$

- *Ejemplo de un escenario simétrico incentivado.* Todos los participantes se consideran parte de un plan de incentivos, es decir, todas las entidades obtienen una rentabilidad positiva al perder el control sobre cada uno de sus elementos de propiedad. La diagonal de la matriz de beneficio B se establece en -1.

$$\text{Benefit matrix } B = \begin{pmatrix} \texttt{BENEF} & val_1 \\ val_2 & \texttt{BENEF} \end{pmatrix}$$

Los siguientes son los beneficios diferenciales para cada entidad participante al ejecutar el protocolo definido por las matrices (3.4):

$$\begin{aligned} &u_0(0) = -1 \\ &u_0(1) = 1 \\ &u_0(2) = 4 \\ &du_0(0,2) = u_0(2) - u_0(0) = 5 \end{aligned} \tag{3.5}$$

$$\begin{aligned} u_1(0) &= -1 \\ u_1(1) &= 4 \\ u_1(2) &= 6 \\ du_1(0,2) &= u_1(2) - u_1(0) = 7 \end{aligned} \tag{3.6}$$

Observen que en este caso el intercambio es beneficiosos para todos los participantes.

- *Ejemplo de un escenario simétrico no incentivado.* Todas las entidades incurren en costos al enviar sus item. En este caso, la diagonal de la matriz de beneficios se establece en 1.

$$\text{Matriz de Beneficios } B = \begin{pmatrix} \texttt{COST} & val_1 \\ val_2 & \texttt{COST} \end{pmatrix}$$

Los siguientes son los beneficios diferenciales para cada entidad participante al ejecutar el protocolo definido por las matrices (3.4):

$$\begin{aligned} u_0(0) &= 1 \\ u_0(1) &= -1 \\ u_0(2) &= 2 \\ du_0(0,2) &= u_0(2) - u_0(0) = 1 \end{aligned} \tag{3.7}$$

$$\begin{aligned} u_1(0) &= 1 \\ u_1(1) &= 6 \\ u_1(2) &= 4 \\ du_1(0,2) &= u_1(2) - u_1(0) = 3 \end{aligned} \tag{3.8}$$

observen que en este escenario, el cambio no se traduce en un beneficio para el participante P_0, mientras que sí es un intercambio rentable para la entidad P_1. Sin embargo, también señalar que P_1 no está motivada para ejecutar el último paso del protocolo, pues pierde beneficio al efectuarlo.Por ese motivo no se da intercambio *racional* desde el punto de vista de la entidad P_1.

- *Ejemplo de un entorno asimétrico.* Para el intercambio, no hay simetría con respecto a los incentivos. La diagonal de la matriz de beneficios

tendrá valores -1 y 1.

$$\text{Matriz de Beneficios } B = \begin{pmatrix} \texttt{COST} & val_1 \\ val_2 & \texttt{BENEF} \end{pmatrix}$$

Los siguientes son los beneficios diferenciales para cada entidad participante, al ejecutar el protocolo definido por las matrices (3.4):

$$\begin{aligned} &u_0(0) = 1 \\ &u_0(1) = -1 \\ &u_0(2) = 2 \\ &du_0(0,2) = u_0(2) - u_0(0) = 1 \end{aligned} \tag{3.9}$$

$$\begin{aligned} &u_1(0) = -1 \\ &u_1(1) = 4 \\ &u_1(2) = 6 \\ &du_1(0,2) = u_1(2) - u_1(0) = 7 \end{aligned} \tag{3.10}$$

En este caso, la entidad P_0, no da lugar a ningún beneficio, por el contrario, para la entidad P_1, el intercambio de items/fichas reporta un beneficio sustancial.

3.1.2. Clasificación atendiendo a Coaliciones

Atendiendo a si existen coaliciones entre los participantes, se propone la siguiente clasificación para distinguir todos los escenarios posibles de intercambio:

Libre de Coalición. Todos los participantes son racionales y ninguno de ellos forman parte de ninguna coalición.

Formalmente se puede representar este tipo de entorno de la siguiente manera:

$$\begin{gathered} \forall i \in \{0, \ldots, v-1\} \quad and \quad \forall j \in \{0, \ldots, m-1\} \\ (h_{i,j}(0) = \texttt{UNKNO}) \wedge \neg(b_{i,j} > 1) \Rightarrow (b_{i,j} = \texttt{COST}) \vee (b_{i,j} = \texttt{NO\_COST}) \end{gathered} \tag{3.11}$$

En otras palabras, la entidad P_i no puede aumentar su pago por la expedición de otros elementos, que no son requeridos por P_i.

Con coaliciones. Formalmente se puede representar este tipo de entorno de la siguiente manera:

$$\begin{gathered}\exists i \in \{0,\ldots,v-1\} \text{ and } \exists j \in \{0,\ldots,m-1\} \text{ s.t.} \\ (h_{i,j}(0) = \texttt{UNKNO}) \wedge (b_{i,j} = \texttt{BENEF})\end{gathered} \tag{3.12}$$

En otras palabras, al menos una entidad P_i es capaz de aumentar su rentabilidad mediante el reenvío de otro item o_j de otra entidad. En este caso, P_i se dice que forma coalición con cada P_K tal que o_j es un item requerido por P_k (es decir, $b_{k,j} > 1$).

Tenga en cuenta que para algunas matrices B seremos capaces de identificar rápidamente la existencia de las intersecciones entre los diferentes coaliciones. Si existe una columna con j en B y dos índices de $i, i' \in \{0,\ldots,1-v\}$, $i \neq i'$, tales que:

$$(h_{i,j}(0) = \texttt{UNKNO}) \quad \wedge \quad (h_{i',j}(0) = \texttt{UNKNO}) \quad \wedge \quad (b_{i,j} = \texttt{BENEF}) \quad \wedge \quad (b_{i',j} = \texttt{BENEF}) \tag{3.13}$$

Entonces, P_i y P_i' formarán dos coaliciones diferentes con P_k, al requerir la entidad P_k el item/ficha o_j.

Tenga en cuenta que, aunque el número total de posibles coaliciones es 2^v, un escenario de intercambio podría ser caracterizado por más de una alianza, y éstos fácilmente se cruzan en cero, uno o más participantes cada vez mayor el número total de posibles escenarios diferentes a 2^{2^v}.

Ejemplos

Para ilustrar la clasificación anterior, se considerará el siguiente ejemplo: un escenario de cuatro entidades, cada entidad en posesión de uno solo producto a cambiar, tal que: P_0 requiere o_3, P_1 requiere o_0, P_2 requiere a o_1 y P_3 requiere o_2. El valor arbitrario *val* es elegido igual para todas las entidades, y representa lo que cada producto vale a cada entidad que lo requiere. Además, consideramos un intercambio simétrico incentivado, es decir, los participantes son incentivados para el intercambio de sus elementos.

Las matrices siguientes define este escenario:

$$\text{Matriz Inicial de Estados} H(0) = \begin{pmatrix} \texttt{ACC} & \texttt{UNKNO} & \texttt{UNKNO} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{ACC} & \texttt{UNKNO} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{UNKNO} & \texttt{ACC} & \texttt{UNKNO} \\ \texttt{UNKNO} & \texttt{UNKNO} & \texttt{UNKNO} & \texttt{ACC} \end{pmatrix}$$

$$\text{Matriz de Beneficios } B = \begin{pmatrix} \texttt{BENEF} & - & - & val \\ val & \texttt{BENEF} & - & - \\ - & val & \texttt{BENEF} & - \\ - & - & val & \texttt{BENEF} \end{pmatrix}$$

- *Ejemplo de un escenario libre de coaliciones.* Ninguno de los participantes es miembro de una coalición con cualquier otra entidad. Por lo tanto, el beneficio de la matriz B será tal que no habrá valores `BENEF` fuera de la diagonal principal.

$$\text{Matriz de Beneficios } B = \begin{pmatrix} \texttt{BENEF} & \texttt{NO\_COST} & \texttt{COST} & val \\ val & \texttt{BENEF} & \texttt{COST} & \texttt{COST} \\ \texttt{NO\_COST} & val & \texttt{BENEF} & \texttt{COST} \\ \texttt{COST} & \texttt{COST} & val & \texttt{BENEF} \end{pmatrix}$$

- *Ejemplo con coaliciones.* Por ejemplo, dos coaliciones son parte del intercambio: P_0 con P_2 y con P_0 P_3, P_1 y P_2 y P_3 no son aliados. La figura 3.1 es una visualización gráfica de estas intersecciones. El siguiente es su representación en la matriz B de beneficios.

$$\text{Matriz de Beneficios } B = \begin{pmatrix} \texttt{BENEF} & \texttt{BENEF} & \texttt{BENEF} & val \\ val & \texttt{BENEF} & \texttt{COST} & \texttt{COST} \\ \texttt{NO\_COST} & val & \texttt{BENEF} & \texttt{BENEF} \\ \texttt{NO\_COST} & \texttt{COST} & val & \texttt{BENEF} \end{pmatrix}$$

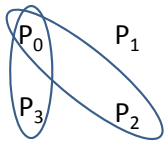

Figura 3.1: Ejemplo con Coaliciones.

3.1.3. Tabla Resumen

La tabla 3.1, resume la taxonomía propuesta detallando las combinaciones de todos los posibles escenarios y sus valores.

Capítulo 4

Imposibilidad del Intercambio Racional

4.1. Resultado de Imposibilidad del Intercambio Racional

El siguiente teorema establece que un intercambio racional no puede existir en ausencia de incentivos y coaliciones entre las entidades participantes.

Teorema 4.1.1. *Sea* $\Pi = \langle P, \mathcal{O}, T \rangle$ *un protocolo de intercambio (tal como se define en la definición 2.1.1) tal que:*

(i) No existen incentivos para ninguna entidad $P_i \in P$ *y*

(ii) No existen coaliciones entre ninguna grupo de entidades de P*,*

Entonces, Π *no es racional.*

Demostración. Supongamos que $\pi = \langle P, \mathcal{O}, T \rangle$ es racional. Sea S^{Π} la matriz que representa el protocolo de π. Además, digamos que $B = [b_{ij}]$ es la matriz beneficio y $H(0) = [h_{ij}(0)]$ es la matriz de estado inicial, que representa el problema de intercambio en la mano.

Sea (stp_t) $P_s \rightarrow P_r : \{o_l\}$, cualquiera de los pasos del protocolo representados en S^{π}, $(t \in \{0, \ldots, n-1\})$.

La ganancia diferencial alcanzada por la entidad remitente P_s después de

ejecutar el paso stp_t se calcula como (ver Definiciones 2.7.1 y 2.7.2):

$$u_s(t+1) = \sum_{\substack{j=0 \\ h_{sj} \neq \texttt{NO\_ACC} \\ j \neq l}}^{m-1} b_{sj} * h_{sj}(t) + b_{sl} * h_{sl}(t+1) \tag{4.1}$$

Tengan en cuenta que, tal como se especifica en la ecuación 2.4, $h_{sl}(t+1) = LOST$ donde $LOST = -1$ entonces tenemos que:

$$\begin{gathered} \forall(stp_t)\ P_s \rightarrow P_r : \{o_l\} \\ u_s(t+1) = u_s(t) - b_{sl} \end{gathered} \tag{4.2}$$

Condiciones (i) y (ii) de este teorema (especificado en las ecuaciones 3.2 and 3.11, respectivamente) se resumen como sigue:

- si $h_{sl}(0) = ACC \Rightarrow b_{sl} = COST$ donde $COST = 1$ (no incentivadas). Esto es $b_{sl} > 0$.
- si $h_{sl}(0) = NO\_ACC \Rightarrow b_{sl} = COST$ donde $COST = 1$ (no incentivadas). Esto es $b_{sl} > 0$.
- si $h_{sl}(0) = UNKOWN \Rightarrow b_{sl} = COST \ \vee \ b_{sl} = NO\_COST \ \vee \ b_{sl} > 1$ (no hay coaliciones). Esto es $b_{sl} \geq 0$.

Por lo tanto, en todos los casos hemos comprobado que $b_{sl} \geq 0$, que se aplica a la ecuación 4.2, podemos concluir que:

$$\begin{gathered} \forall(stp_t)\ P_s \rightarrow P_r : \{o_l\} \\ u_s(t+1) = u_s(t) - b_{sl} \leq u_s(t) \end{gathered} \tag{4.3}$$

Por lo tanto:

$$\begin{gathered} \forall(stp_t)\ P_s \rightarrow P_r : \{o_l\} \\ du_s(t, t+1) \leq 0 \end{gathered} \tag{4.4}$$

Entonces:

$$du_s(0, n) \leq 0 \tag{4.5}$$

En contradicción con la definición de protocolo racional dada en la sección 2.8. □

Capítulo 5

Entorno de Aplicación

5.1. RCI

En 1974, la empresa RCI fue pionera en el concepto de las vacaciones mediante intercambio. Desde entonces, millones de propietarios de tiempo compartido han descubierto que una suscripción a RCI realmente mejora la calidad de la propiedad vacacional.

Hoy en día, RCI cuenta con más de tres millones de miembros en todo el mundo, que disfrutan de vacaciones con más de 3.700 complejos afiliados. Los miembros de RCI pueden beneficiarse de los conocimientos, la experiencia y los recursos de RCI. Guías que prestan asistencia en la planificación de las vacaciones de cambio, edición de unos directorios con los complejos afiliados que envían junto con otra información a sus miembros. Además tienen paginas web donde se pueden visualizar los directorios.

¿Qué es la Multipropiedad o el Tiempo Compartido?

Es un nuevo concepto de vacaciones, el propietario no tiene un inmueble propiamente dicho, sino que se venden los intereses de una propiedad vacacional en intervalos de una semana. Las propiedades pueden ser apartahoteles, hoteles, residenciales, bungalows, etc. y el propietario posee, en régimen compartido con otros socios, la posesión de dicha propiedad en intervalos de tiempo. De esta forma se puedan utilizar para reservar e intercambiar alojamientos turísticos. La cuota de los miembros, después de la compra inicial, da posibilidad al intercambio entre los socios.

¿Por qué ser dueño de Tiempo Compartido?

Con la propiedad de vacaciones por intervalos, los consumidores tienen la

oportunidad de comprar alojamiento de calidad, que ofrecen una gran variedad de servicios en populares destinos nacionales e internacionales, que no podrían alcanzarse si se tuvieran que comprar en su totalidad.

El costo de un tiempo compartido en gran medida depende de la ubicación, el tamaño de la unidad y la temporada, pero siendo mucho menor que el de una propiedad unifamiliar. Hoy en día el promedio de tiempo compartido se vende por aproximadamente 10.000 .

¿Por qué utilizar RCI?

La ventaja de la Multipropiedad o Tiempo Compartido consiste en poder disfrutar de diferentes vacaciones cada vez, sin un gasto excesivo comparado con el modelo tradicional. Para usar estos servicios, el propietario de una Multipropiedad o Tiempo Compartido tiene que afiliarse y pagar una cuota de membresía anual (los primeros años suelen estar incluidos en el contrato de compra). Por cada intercambio confirmado se cobra una cuota de intercambio. Hay otras cuotas como el certificado de huéspedes o upgrade (cambiar a una unidad mas grande) o semanas extras.

¿Cuál es la Cuota de Socio?

La cuota varía para los distintos países, dependiendo del continente al que pertenecen (por el número de complejos existente en cada uno de ellos). Para este año 2011 la previsión para Europa es de:

- 1 año: 175€.
- 3 años: 370€.
- 5 años: 555€.

según las distintas modalidades.

Además existen diversas cuotas por diversos tipos de intercambio (un ejemplo es cuando se realizan entre complejos de distintos continentes). También hay ofertas de semanas que no tienen intercambios previstos en el próximo mes, y cuyos propietarios depositaron para aumentar su *Poder de Intercambio* (Dibujo 5.1) y por lo tanto RCI las va a perder como negocio .

¿Cómo se realiza el intercambio?

Se pueden depositar las semanas hasta 2 años antes de su fecha y sacar otra semana hasta 1 año después de esta fecha. El principio para el intercambio se

basa en que se pueden realizar a complejos con valor similar. Esto se conoce como Poder de Intercambio. Este valor depende de las siguientes situaciones:

Cuando un usuario es dueño de una semana en este sistema y decide depositar su semana de vacaciones en RCI para poder intercambiarla por otra, en el momento de realizar el depósito, RCI le asigna un valor a su semana vacacional, el cual se calcula respondiendo a las siguientes preguntas:

1. Clasificación - ¿Qué fue lo que el usuario depositó?
2. Demanda - ¿Cuántos socios RCI buscan una unidad vacacional como la que el usuario depositó?
3. Inventario - ¿Cuántos depósitos similares tenemos en existencia?
4. Utilización - ¿Cuántos depósitos como el suyo han sido confirmados por otros socios RCI en el pasado?
5. ¿En qué temporada se encuentra ubicada su semana?
6. ¿Cuál es el tipo y tamaño de su unidad?
7. ¿Con cuánto tiempo de anticipación a la fecha de su viaje esta realizando el depósito?

Cuando realizamos el depósito, realizamos nuestra petición sobre los complejos existentes, en las fechas que a nosotros nos interesa, eligiendo ver todas las semanas que se encuentren disponibles en el Sistema de Intercambio RCI®Weeks en ese momento. Si se elige ver todas las semanas disponibles, también encontrará semanas vacacionales que requieren de un mayor Poder de Intercambio que el de los depósitos que se tengan disponibles. Se calcula el valor de dicha solicitud comprobando que es igual al Poder de Intercambio que nosotros tenemos. En caso afirmativo se produce el intercambio. La clave para realizar un intercambio exitoso depende de:

1. Depositar con anticipación.
2. Solicitar un intercambio similar a lo que el usuario depositó.

¿Qué ocurre en caso contrario? Si nuestro Poder de Intercambio es menor o mayor procedemos de la siguiente manera:

Figura 5.1: Poder de Intercambio. Fuente: RCI

Figura 5.2: Saldo de Intercambio. Fuente: RCI

Si el socio contaba con un mayor Poder de Intercambio, recibirá Saldo de Intercambio (Dibujo 5.2) por la diferencia que haya quedado al restar su semana depositada menos la solicitada.

Este saldo residual podrá unirse a otras semanas que usted poseyera, para realizar otro intercambio. En caso de que el Poder de Intercambio sea menor entonces tendrá que combinar su Saldo de Intercambio con otra semana vacacional que haya Depositado, y de esta manera incrementar el Poder de Intercambio de su Depósito.

En todos los casos, cuando se produce un intercambio, la empresa RCI reserva cada semana intercambiada a los nuevos clientes. La notificación se realiza a la base de datos de las propiedades, accediendo a nuestras

Figura 5.3: Acumulación de Poder de Intercambio. Fuente: RCI

vacaciones gracias a la recepción de dichos alojamientos, mediante un código proporcionado por RCI, que funciona como reserva de dicha semana vacacional.

En el caso de que una semana haya sido depositada y RCI no consiga socio para su disfrute, la empresa pierde el valor de dicho intercambio, pero nunca el cliente que la depositó.

5.1.1. Intercambios Vacacionales Racionales

RCI actúa como una TTP en el caso de los intercambios vacacionales entre usuarios. En nuestro marco teórico es posible prescindir de dichas TTP. El entorno RCI puede desplegarse en la red de manera que los usuarios obtienen el mismo beneficio vacacional, pero además sin los costes añadidos por los intermediarios. Pensamos que dicha empresa podría proporcionar un entorno apropiado al resultado obtenido teóricamente, y por lo tanto crear intercambios múltiples de forma racional. En un principio, hemos tenido que restringir el volumen de intercambios, así como las complejidades múltiples que un empresa de tal tamaño y experiencia de RCI ofrecia a sus clientes.

En nuestro caso el entorno que vamos a utilizar sería el siguiente:

- El número de entidades en el que nos hemos basado para crear nuestro

entorno es de 15 entidades con el mismo número de items/fichas por intercambiar.(Esto nos sirve como prototipo, ya que un número mayor de entidades sería difícil de visualizar)

- Cada entidad tiene que ceder para el intercambio, el mismo número de item/fichas que solicita.
- Cada item/fichas es una semana de intercambio en un complejo vacacional concreto.
- Los intercambios se van a producir en el mismo periodo de tiempo (en nuestro caso un mes concreto), y nuestros complejos los vamos a valorar todos iguales, por lo que el Poder de Intercambio será el mismo.
- Dos entidades nunca pueden tener un mismo item/fichas desde el inicio.
- Dos entidades no pueden solicitar un mismo item/fichas como resultado final.
- Cada entidad es un socio.
- El periodo para depositar los periodos vacacionales se restringen. Nadie puede depositar cuando queden menos de 3 meses para el intercambio (tiempo estimado para una preparación aceptable de las vacaciones), y se puede depositar un año antes, como mucho.
- Una vez depositado un periodo vacacional, este no puede ser retirado.
- El orden de petición de los intercambios se realiza, primando al que primero deposita su periodo vacacional. El último en elegir será el que más tarde depositó su periodo vacacional.
- Una vez enviado el listado de prioridades, todo socio tiene que aceptar el intercambio que se le asigne, haga o no uso de la unidad vacacional que le sea asignada.
- El acceso al periodo vacacional es con clave numérica proporcionada por el cliente o socio (dicha clave puede ser de acceso directo a un apartamento o proporcionar unas llaves en una conserjería de un apartahotel).

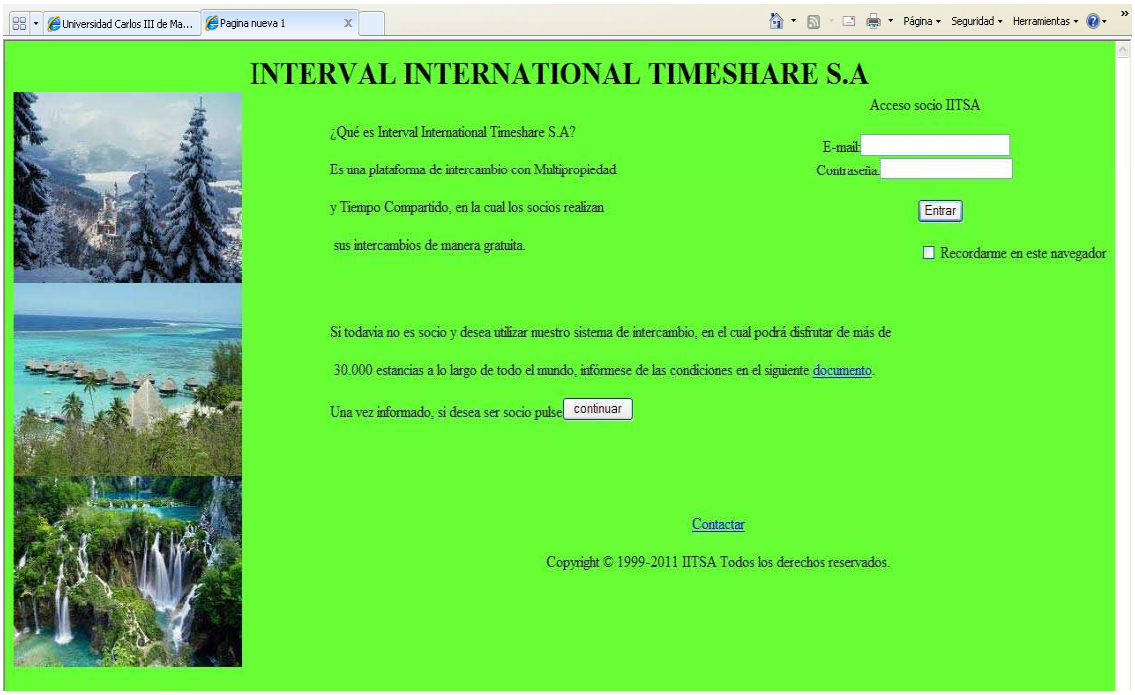

Figura 5.4: Pantalla inicial de la aplicación web IITSA.

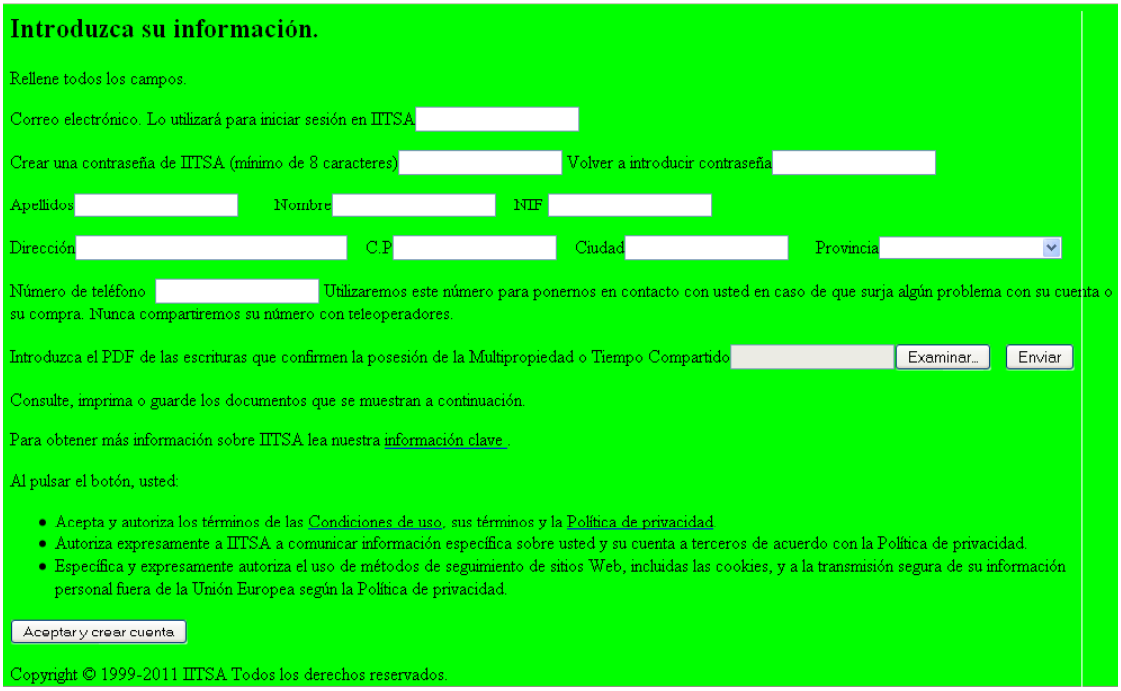

Figura 5.5: Formulario de Registro en la aplicación web IITSA.

El funcionamiento será el siguiente:

- Cada socio tendrá que registrarse la primera vez, para comprobar que posee el periodo vacacional, del cual dice ser propietario. Se le dará un número de socio así como un código por cada periodo vacacional que posea.

- Cuando decida depositar un periodo vacacional, tendrá que introducir el número de socio y el código del periodo. El sistema, gracias al registro, sabe donde está localizada la unidad vacacional de cada código introducido. Ejemplos de pantallas de la aplicación web que hemos denominado IITSA (Interval International Timeshare S.A), Dibujo 5.4 y Dibujo 5.5 referidos a la página principal y al formulario de registro de cliente.

- 3 meses antes del intercambio, se envían todos los periodos vacacionales depositados para dicha fecha. En ese momento se crea la Matriz H de estado. Así como el número de orden que el cliente tiene en la elección. En un tiempo de 3 días han de reenviar dicha lista con una ordenación por prioridades de los periodos vacacionales. Si alguien no lo envía, queda el último en el orden de prtición.

- El sistema con las peticiones y el número de orden de cada socio, crea la Matriz B de beneficio.

- Hacemos ejecutar la aplicación, cuando obtenemos el protocolo empezamos el intercambio entre los socios. La manera de actuar sería:

    1. El sistema manda un e-mail al socio-enviador con los periodos vacacionales que tiene que enviar al socio-receptor. Se enviarán las claves de acceso al periodo vacacional.
    2. Cuando el socio-receptor obtiene las claves de acceso envía al sistema un e-mail de OK para continuar con el resto de los pasos.

- Para todo esto, la aplicación ha mandado un e-mail a todos los socios para que este intercambio se realice en una fecha concreta y periodo concreto (si la aplicación da un tiempo de 3 días para devolver la lista de prioridades, un día en ejecutarse y obtener el protocolo, se mandará con

el e-mail de la lista de periodos vacacionales que 5 días después de la recepción de este mensaje se procederá al intercambio, atento a su correo)

- Una vez recibido OK de un socio-receptor, enviamos el siguiente mensaje del protocolo, así sucesivamente hasta terminar con todos los pasos del protocolo.

Todos los pasos se realizarán, puesto que el protocolo generado es racional (por definición los participantes de este protocolo obtendrn mejores beneficios cuando no se desvían del protocolo).

Todo este proceso duraría una semana, por lo que cuando quedan dos meses y medio para nuestras vacaciones hemos obtenido nuestro periodo vacacional señalado.

La aplicación se ejecutaría al principio de cada mes, con los periodos vacacionales que están depositados con tres meses a la fecha de ejecución.

En la siguiente sección veremos un ejemplo concreto .

5.1.2. Ejemplo de Intercambio

La aplicación que hemos creado se ejecuta por línea de comandos, al ser un motor de intercambio no necesita de un interface de usuario.

- El ejecutable que nombra a la aplicación le hemos llamado RCI_IITSA.EXE, al cual le acompañan dos archivos de texto como parámetros.
- El primer parámetro sería un archivo de texto donde aparecen
  - El número de entidades
  - El número de item/fichas
  - El número de mensajes a intercambiar
  - Las tres matrices, la de Estado, la de Beneficio y la de Relaciones.
- El segundo parámetro nos mostraría el resultado final del protocolo de intercambio multiparte, que lo guardaremos en un archivo de texto.

La aplicación lo primero que hace es mostrar todo lo especificado en el archivo de texto que le pasamos como primer parámetro (Figura 5.6), en nuestro ejemplo el parametro es Exp1_5_10.txt, un archivo con :

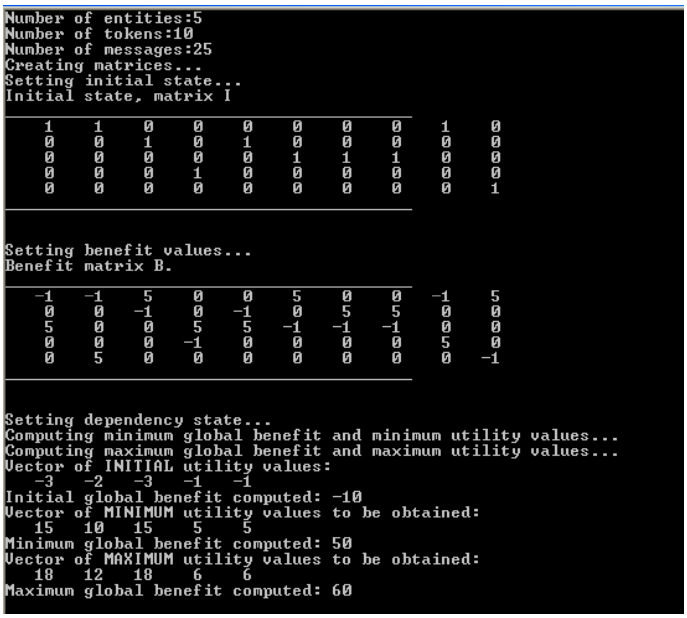

Figura 5.6: Ejemplo de pantalla inicial de la aplicaciń RCI_IITSA.EXE.

- Número de entidades igual a 5.
- Número de tokens igual a 10
- Número de mensajes a intercambiar en el protocolo es de 25.
- Las tres matrices, la de Estado, la de Beneficio y la de Relaciones (por la naturaleza del problema dicha matriz de Relaciones la obviamos).

La primera matriz que aparece es la de Estado y su significado es el siguiente:

- Las filas son entidades definidas desde la P_0 hasta la P_{n-1}.
- Las columnas son los item/fichas desde o_0 hasta o_{k-1}.
- La celda que tiene un 1 significa, que la entidad correspondiente a esa fila, posee el item/ficha correspondiente a dicha columna.

En nuestro caso lo vamos a mostrar de la siguiente manera (Figura 5.7), para una mejor comprensión del ejemplo:

La segunda matriz en aparecer es la de Beneficio, y su formación en filas y columnas es igual que la anterior. Ahora los números cambian.

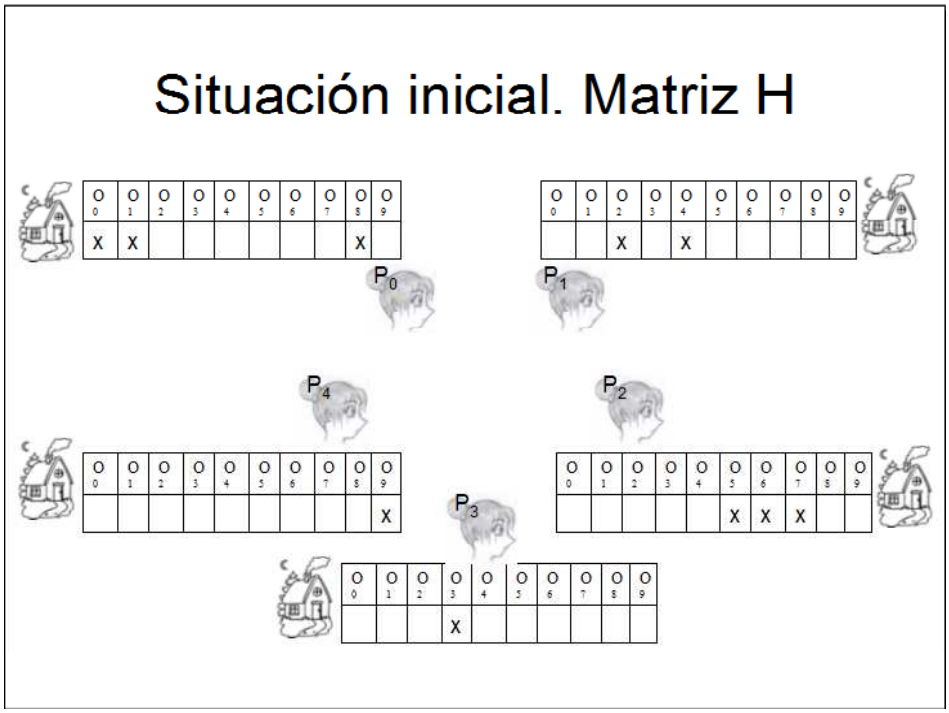

Figura 5.7: Identificación de los valores de la matriz H de la aplicación.

- Un -1 en una celda indica que la entidad de esa fila pierde beneficio si cede el item/ficha de esa columna.
- Un 5 en una celda indica que la entidad de esa fila requier el item/ficha de esa columna y lo valora con un valor arbitrario val=5.

En nuestro ejemplo la disposición final tras ejecutar el protocolo de intercambio quedaría de la siguiente forma (para una ilustración gráfica ver Figura 5.8).

Comprobamos que cada entidad pierde el mismo número de item/fichas que los que recibe. Además sabemos por la demostración del resultado, que todos van a obtener el item/ficha que solicitaron.

Seguidos a estas dos matrices aparecen una serie de parámetros que se explicarán a continuación:

- Primero se realiza el cálculo de los dos beneficios globales, tanto el mínimo como el máximo.
- Vector de beneficio inicial, la suma de los -1 de cada fila en la matriz

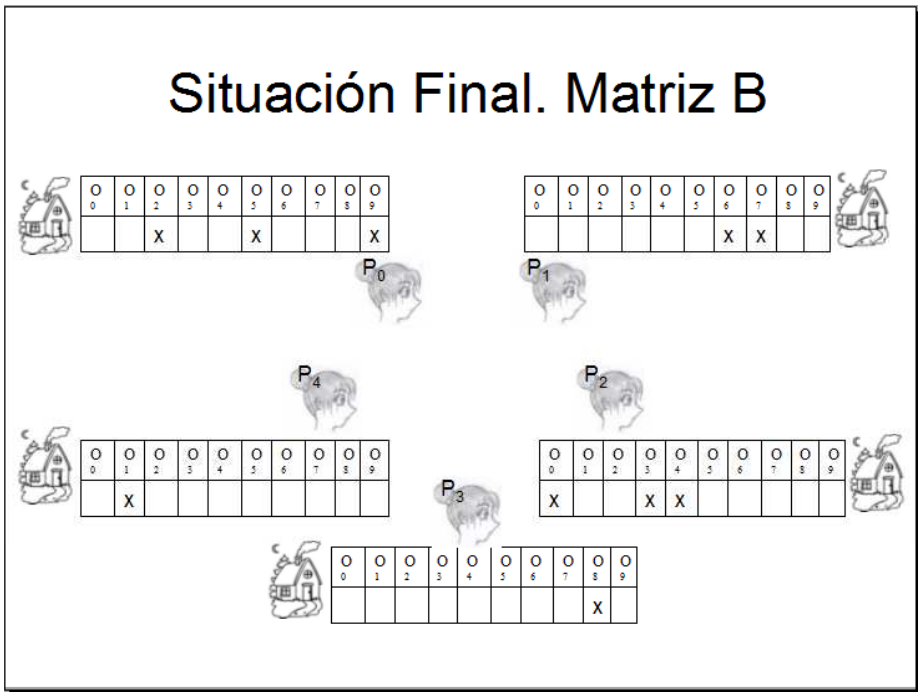

Figura 5.8: Identificación de los valores de la matriz B de la aplicación.

matriz B de beneficio (hace referencia a los tokens que cada entidad va a perder al final del protocolo).

- Vector de utilidad mínimo, es el valor mínimo que quiere conseguir cada entidad para realizar el intercambio. Se calcula como la suma de los 5 de cada fila en la matriz matriz B de beneficio (hace referencia a los tokens que cada entidad va a obtener al final del protocolo).

- Valor mínimo de beneficio entre todas las entidades, es la suma de todos los valores del vector anterior.

- Vector de utilidad máximo, es el valor máximo que quiere conseguir cada entidad para realizar el intercambio. Se calcula aplicando las ecuaciones 2.8.

- Valor máximo de Beneficio entre todas las entidades, es la suma de todos los valores del vector anterior. Va a ser el valor que busque nuestro algoritmo, y cuando lo alcance, nos presentará la solucin obtenida, y por lo tanto el protocolo de aplicación.

Una vez que aparecen estos parámetros la aplicación comienza a buscar soluciones.

5.2. Algoritmo de Búsqueda

5.2.1. Simulated Annealing

Simulated annealing (SA) es un algoritmo de búsqueda meta-heurística para problemas de optimización global. El objetivo general de este tipo de algoritmos es encontrar una buena aproximación al valor óptimo de una función en un espacio de búsqueda grande. El nombre deriva del proceso de recocido del acero y cerámicas, una técnica que consiste en calentar y luego enfriar lentamente el material para variar sus propiedades físicas. El calor causa que los átomos aumenten su energa y que puedan así desplazarse de sus posiciones iniciales (un mínimo local de energía); el enfriamiento lento les da mayores probabilidades de recristalizar en configuraciones óptimas.

5.2.2. Parámetros del Algoritmo

En la Figura 5.9 los datos que nos aparecen por pantalla serían:

- Trial number, es el número de intentos que se van a realizar. Nosotros nos decidimos por 5 trial, y que de entre ellos se buscara la mejor solución posible.
- Fecha y Hora de comienzo de cada Trial (para conocer el tiempo de búsqueda).
- $T_0 = 0{,}430000$ es la Temperatura inicial con que comienza a ejecutarse el algoritmo. Al comienzo de cada ciclo de búsqueda, la temperatura se reduce un tanto por ciento. Esta reducción se introduce como dato en el programa.
- CurrFitness, es el valor de beneficio global de todas las entidades, cuando supera el valor mínimo calculado para todas las entidades, se ha encontrado una solución.
- BestFitness, nos muestra cuál ha sido el mayor beneficio global de todas las entidades hasta el momento.

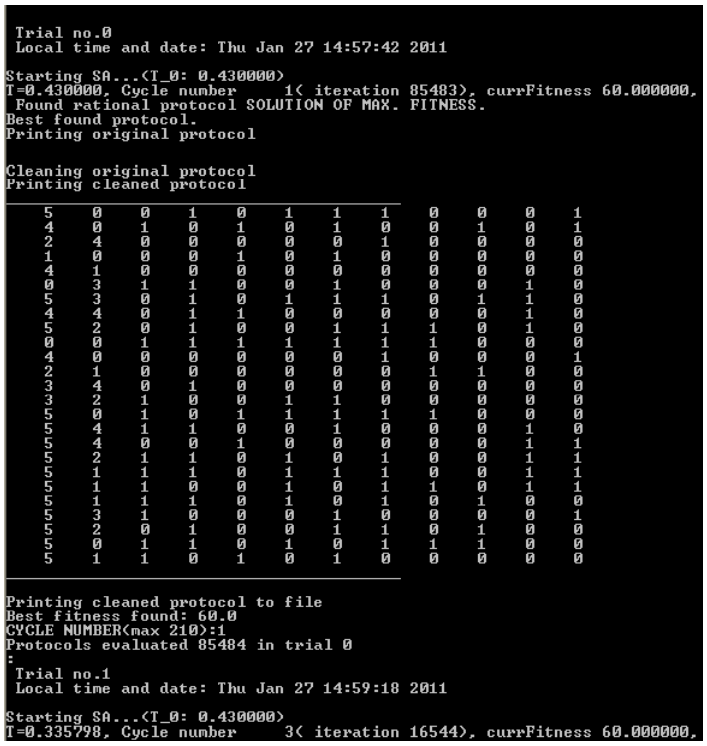

Figura 5.9: Salida de una solución del protocolo en la aplicación

Cuando se encuentra la solución limpiamos las líneas inválidas del protocolo generado y lo mostramos por pantalla.

En la aplicación, después de la matriz de protocolo, se nos muestra otra serie de parámetros que son:

- Número de Ciclo, relaciona el número de ciclos que tenemos para encontrar la solución, con el número en el que se ha conseguido.
- Protocolos evaluados en cada ciclo, en nuestra aplicacón estamos probando 1.000.000 soluciones posibles por ciclo. Nos indica en qué lugar de cada ciclo encontró la solución.
- Comienzo del siguiente Trial.

Según van aumentando el número de entidades, de item/fichas o de mensajes intercambiados, la matriz de Protocolo es menos manejable, y ya a simple vista, bastante poco tratable. Por ello una de las modificaciones de la aplicación fue sacar mediante el segundo parámetro, un archivo con el resultado

ya limpio y muy manejable para posteriores manipulaciones. En este caso el archivo SOL5_10.TXT nos da por salida lo siguiente:

$P_0 \rightarrow P_4 : \quad o_1$
$P_0 \rightarrow P_3 : \quad o_8$
$P_4 \rightarrow P_0 : \quad o_9$
$P_1 \rightarrow P_2 : \quad o_4$
$P_3 \rightarrow P_0 : \quad o_3$
$P_2 \rightarrow P_1 : \quad o_5, o_6, o_7$
$P_1 \rightarrow P_0 : \quad o_2, o_5$
$P_0 \rightarrow P_2 : \quad o_0, o_3$
Number of entities: 5
Number of tokens: 10
Number of messages: 25

Donde se nos va indicando la entidad que envía, la que recibe y los items/fichas que recibe.

Cada paso del protocolo lo explicaremos de la siguiente forma. Partiendo del estado actual cogeremos una a una las líneas del protocolo generado. Vamos a utilizar el primer paso del protocolo que estamos utilizando como ejemplo que es:

$P_0 \rightarrow P_4 : \quad o_1$

El protocolo nos indica que tenemos que enviar el item/ficha o_1 perteneciente a la entidad P_0, a la entidad P_4. Dicho movimiento lo hemos representado gráficamente en las Figuras 5.10 y 5.11.

Cuando finalizamos la aplicación, pues hemos encontrado la solución buscada, aparecen otra serie de parámetros, alguno de ellos estadísticos y de resumen final (Figura 5.12. Estos son:

- SA_IC_MAX: número máximo de ciclos de busqueda.
- SA_NUMBER_MOVES: número de soluciones buscadas en cada ciclo
- SA_MAX_FAILED_CYCLES: número de ciclos con fallo para producir error.
- SA_COOLING_RATE: tanto por ciento de disminución de la temperatura por ciclo.
- SA_TEMP: Temperatura inicial.

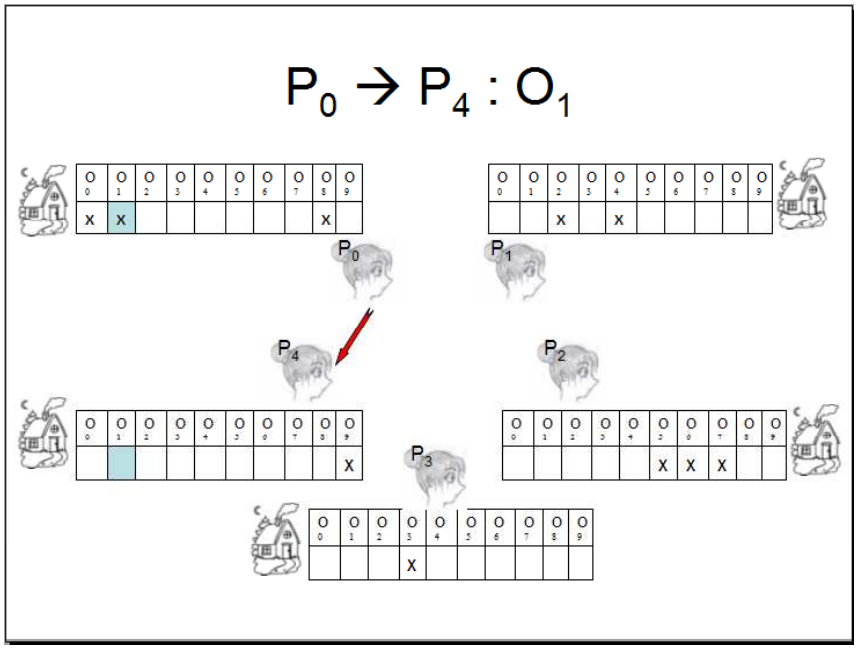

Figura 5.10: Representación del inicio de un paso del protocolo.

- MAX_NO_OF_MESSAGES: número de mensajes del protocolo de intercambio.
- NUMBER OF TRIALS: número de protocolos a encontrar.
- NUMBER OF ENTITIES: número de entidades.
- Número de protocolos evaluados en los 5 trial
- Desviación estándar.
- La solución más rápida evaluada dentro de cada trial.
- La solución más tardía encontrada.
- Número de protocolos con éxito.
- Tanto por uno de éxitos.
- Fecha y Hora de finalización de la aplicación.

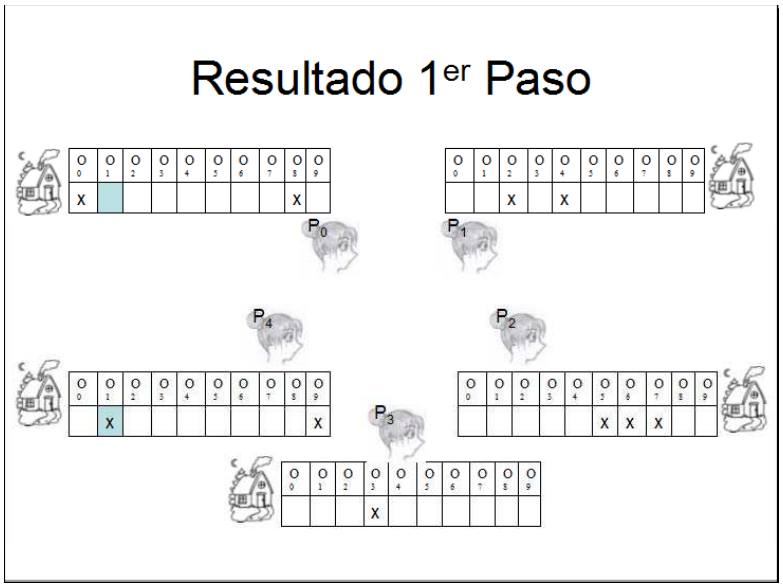

Figura 5.11: Representación del final de un paso del protocolo.

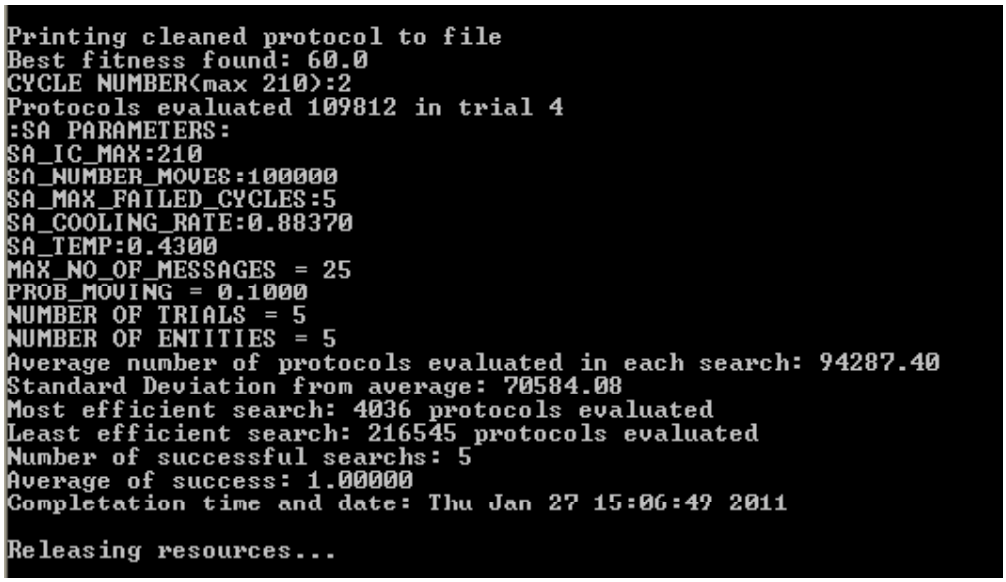

Figura 5.12: Parámetros finales de la aplicación

Capítulo 6

Conclusiones

6.1. Conclusiones

El formalismo descrito en este trabajo para la descripción y síntesis automática de protocolos de intercambio racional, nos ha permitido representar factores tradicionalmente considerados muy complejos. Cuestiones tales como los grupos de coaliciones de entidades o programas de incentivos son fáciles de definir ahora y además se encontró un modelo para describirlas. Este trabajo nos proporciona una taxonomía simple, según la cual, protocolos de intercambio racional complejos pueden ser fácilmente clasificados. Por último, la clasificación nos ha permitido establecer un resultado importante: la imposibilidad de intercambio racional entre entidades ante la ausencia de incentivos o de grupos de coaliciones. En otras palabras, la cooperación entre las entidades egoístas solo puede surgir mediante la presencia de factores externos.

Por otro lado, no quisimos quedarnos en un resultado solo teórico, sino que buscamos una aplicacón práctica de lo obtenido. La cantidad de servicios que hoy en día necesitan de protocolos de seguridad para intercambios es cada vez mayor (como ejemplo la banca digital, comercio electronico, etc). Buscamos un entorno de aplicación en redes ad hoc o P2P, y con ayuda de una herramienta, pudimos obtener resultados prácticos.

Hemos tenido que parar en algún momento de realizar estos experimentos, y en este proyecto hemos visto, como ejemplo, uno de ellos.

6.1.1. Trabajos Futuros

Son interesantes como punto de partida para posibles líneas de investigación los siguientes puntos:

- Aumentar el número de entidades y item/fichas en los experimentos.
- Reducir el número de restricciones que aplicamos a nuestro entorno (definidas en el punto 6.1) . Esto nos acercaría más a un problema real, como el que se le plantea a la empresa RCI.SA.

6.1.2. Publicaciones

El resultado teórico de este proyecto ha sido presentado para su publicación:

Manuscript Number:	TCS-D-10-00241
Manuscript Title:	On the Impossibility of Rational Exchange without Incentives or Coalitions
Author(s):	Almudena Alcaide, Ph.D.; Roman Almendros Gines; Arturo Ribagorda, Ph.D.
Submitted to:	Theoretical Computer Science

Apéndice A

Presupuesto del Proyecto

A.1. Valoración Económica del Proyecto

La valoración económica del proyecto la vamos a realizar bajo la premisa de que dicho proyecto es un estudio teórico. En un principio, no se va a lanzar la aplicación a la red y, por lo tanto, no se contempla su comercialización, por lo que los parámetros económicos a los que tendríamos que hacer referencia se ven mucho más limitados.

Por ello, no mencionaremos el gasto en infraestructuras que necesitaríamos para montar una empresa de este volumen de negocio, que intenta competir con la mayor empresa de intercambio vacacional y con su dilatada trayectoría y experiencia.

En este punto, nos vamos a centrar en el coste económico del trabajador que ha realizado dicho proyecto.

Dada la naturaleza multidiciplinar del trabajo a realizar, la formación matemática del proyectista (licenciado en Matemáticas por la Universidad Complutense de Madrid) ha sido determinante para la consecueción de los objetivos que se plantearon al inicio de este proyecto. Esto incrementa significativamente el coste total de personal y así se han realizado los siguientes cálculos en base al número total de 300 horas invertidas.

A.1.1. Fases del Proyecto

El proyecto ha tenido tres fases diferenciadas. La estimación del tiempo se ha realizado sumando los tiempos anotados en el *Cuaderno de Trabajo* del

proyecto.

Tarea	**Porcentage del tiempo total**	**Número de horas**
Estado del arte	30 %	90h
Resultado de Imposibilidad	30 %	90h
Desarrollo del entorno Mejora de la aplicación Realización de experimentos	30 %	90h
Realización de la memoria Preparación defensa	10 %	30h

A.1.2. Coste de Personal

El salario bruto estipulado para un trabajador de estas caracteristicas (doble licenciatura) sería de 42,000€anuales (28,000€netos) repartidos en 14 pagas.

Calculamos para este trabajador la siguiente información:

- Un trabajador realiza por convenio al año, un total de:

$$46\ semanas\ *\ 35\ horas = 1{,}610\ horas\ anuales$$

- El coste bruto de hora sería:

$$42{,}000\ euros\ brutos\ /\ 1{,}610\ horas\ anuales = 26,08\ euros/hora$$

- Que en coste neto se reduciría a:

$$28{,}000\ euros\ netos\ /\ 1{,}610\ horas\ anuales = 17,39\ euros/hora$$

Aplicado sobre las 300 horas invertidas, obtendriamos un coste de:

$$26,08 euros\ *\ 300\ horas = 7{,}824 euros$$

Repartidos en:

- Sueldo neto: 17,39€ * 300 horas= 5.217€.
- Impuestos del trabajador: 2.607€.

A.1.3. Coste de Material

El trabajo ha sido realizado en dos equipos infomáticos:

- Portátil HP 530, procesador Celeron M410, 1.60GHz con disco duro serial ATA de 120Gb y DDR II SDRAM de 512 MB.
- Ordenador PC ADL P4 , procesador intel, 2.4GHz con disco duro de 200Gb.

Basándonos en un amortización anual del 25 % y la suma del coste de los equipos de 995€, el importe total de material hardware se eleva a 46,35€.

A.1.4. Coste Total

La suma de ambas cantidades es de 7,870, 35€.

Bibliografía

[Abadi et al., 2002] Abadi, M., Glew, N., Horne, B., and Pinkas, B. (2002). Certified email with a light on-line trusted third party: Design and implementation. In *Proceedings of 2002 International World Wide Web Conference*, pages 387–395.

[Alcaide, 2009] Alcaide, A. (2009). Rational exchange protocols. Technical report, University Carlos III of Madrid. Computer Science Department. Spain. Ph.D. Thesis.

[Alcaide et al., 2006] Alcaide, A., Estévez-Tapiador, J., Hernández Castro, J., and Ribagorda, A. (2006). Rational exchange– a formal model based on game theory. In *Proceedings ETRICS'06*. Springer-Verlag. LNCS Vol. 3995/2006, pp. 396-408.

[Alcaide et al., 2007] Alcaide, A., Estévez-Tapiador, J., Hernández Castro, J., and Ribagorda, A. (2007). Bayesian rational exchange. *International Journal of Information Security*, 1(1):1615–13.

[Alcaide et al., 2008a] Alcaide, A., Estévez-Tapiador, J., Hernández Castro, J., and Ribagorda, A. (2008a). Automated synthesis of multiparty rational exchange security protocols. *International Transactions on Systems Science and Applications, special issue on Complex Negotiation and Scheduling in Multi-Agent Systems*, 4(4):312–321.

[Alcaide et al., 2008b] Alcaide, A., Estévez-Tapiador, J., Hernandez Castro, J., and Ribagorda, A. (2008b). Nature-inspired synthesis of rational protocols. In *Proceedings of the 10th International Conference On Parallel Problem Solving from Nature (PPSN 2008)*. LNCS Vol. 5199, pp. 981–990.

[Asokan et al., 1997] Asokan, N., Schunter, M., and Waidner, M. (1997). Optimistic protocols for fair exchange. In *4th ACM Conference on Computer and Communications Security*, pages 8–17.

[Asokan et al., 1998] Asokan, N., Shoup, V., and Waidner, M. (1998). Asynchronous protocols for optimistic fair exchange. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 86–99.

[Aumann, 1959] Aumann, R. J. (1959). Acceptable points in general cooperative n-person games. *Contributions to the Theory of Games IV, Annals of Mathematics Study*, 40:287–324. Princeton University Press, Princeton, NJ.

[Aumann, 1960] Aumann, R. J. (1960). Acceptable points in games of perfect information. *Pacific Journal of Mathematics*, 10:381–417.

[Aumann, 1961] Aumann, R. J. (1961). The core of a cooperative game without side payments. *Transactions of the American Mathematical Society*, 98:539–552.

[Bahreman and Tygar, 1994] Bahreman, A. and Tygar, J. (1994). Certified electronic mail. In *Proceedings of 1994 Symposium on Network and Distributed System Security*, pages 3–19.

[Buttyán, 2001] Buttyán, L. (2001). Building blocks for secure services: Authenticated key transport and rational exchange protocols. Technical report, Swiss Federal Institute of Technology. Lausanne (EPFL). Ph.D. Thesis No. 2511.

[Buttyán and Hubaux, 2001] Buttyán, L. and Hubaux, J. (2001). Rational exchange– a formal model based on game theory. In *Proceedings 2nd International Workshop on Electronic Commerce*. Springer-Verlag. LNCS Vol. 2232, pp. 114.

[Maynard-Smith and Price, 1973] Maynard-Smith, J. and Price, G. (1973). The logic of animal conflict. *Nature*, 246:15–18.

[Pagnia and Gärtner, 1999] Pagnia, H. and Gärtner, F. (1999). On the impossibility of fair exchange without a trusted third party. Technical

report, Darmstadt University of Technology, Department of Computer Science.

[Palomar et al., 2007] Palomar, E., Alcaide, A., Estévez-Tapiador, J., and Hernández-Castro (2007). Bayesian analysis of secure p2p sharing protocols. In *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS (2)*, pages 1701–1717.

[Syverson, 1998] Syverson, P. (1998). Weakly secret bit commitment: Applications to lotteries and fair exchange. In *Proceedings of the 11th IEEE Computer Security Foundations Workshop*, pages 2–13.